



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/807,824

04/18/2001

Tomoyuki Asano

09812.0501

6164

22852

7590

11/28/2008

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP

901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER

CHEN, SHIN HON

ART UNIT

PAPER NUMBER

2431

MAIL DATE

DELIVERY MODE

11/28/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 09/807,824	Applicant(s) ASANO ET AL.	
	Examiner SHIN-HON CHEN	Art Unit 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 March 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7, 9-15, 17-37, 39-45, 47-69, 71-73, 75-90 and 138-157 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7, 9-15, 17-37, 39-45, 47-69, 71-73, 75-90, and 138-157 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-7, 9-15, 17-37, 39-45, 47-69, 71-73, 75-90, and 138-157 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-7, 9-15, 17-37, 39-45, 47-69, 71-73, 75-90, and 138-157 are rejected under 35 U.S.C. 102(b) as being anticipated by Traw et al. U.S. Pat. No. 5949877 (hereinafter Traw).

4. As per claim 1, Traw discloses a data transmitting system comprising a portable data recording medium and a drive unit which accesses the portable data recording medium,

the portable data recording medium including:

a security module comprising a nonvolatile memory which executes a mutual authentication protocol with the drive unit (Traw: figure 3: the content source has authentication and key exchange subsystem 304/security module associated with it; column 9 lines 31-38); and

a storage area distinct from the security module (Traw: figure 3: the content source/storage area distinct from the subsystem 304; column 2 lines 61-65: the devices that include non-volatile memories for storing contents); and
the drive unit including:

Art Unit: 2431

a controller which executes the mutual authentication protocol when accessing the portable data recording medium (Traw: figure 4: the content destination authentication subsystem 404/controller; figure 9 lines 31-39); and

an interface unit which accesses the storage area of the data recording medium (Traw: figure 4: content destination accesses the content through bus).

5. As per claim 2, Traw discloses the system as set forth in Claim 1. Traw further discloses wherein the mutual authentication protocol uses public-key encryption technology (Traw: figure 3 and figure 4: both subsystems utilize public key infrastructure and use public key certificates).

6. As per claim 3, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the storage area is a disc (Traw: column 3 lines 25-34: the storage devices such as disk drives).

7. As per claim 4, Traw discloses the system as set forth in claim 3. Traw further discloses wherein the drive unit further includes means for driving the disc (Traw: column 3 lines 25-34).

8. As per claim 5, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the interface unit accesses the storage area directly (Traw: figures 3 and 4: the 1394 bus that connects the content source and content destination).

Art Unit: 2431

9. As per claim 6, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the storage area is a memory chip (Traw: column 2 lines 35-45).

10. As per claim 7, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the interface unit accesses the storage area via the security module (Traw: figures 3 and 4: the content and destination is connected through bus and authentication subsystems).

11. As per claim 9, Traw discloses the system as set forth in claim 1. Traw further discloses wherein identification data of the portable data recording medium is stored in the security module (Traw: figure 3 and 4: the subsystems/security modules include certificates; column 6 lines 25-27: the certificates include unique device ID).

12. As per claim 10, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the security module stores a revocation list of illegal drive units (Traw: figures 3: both subsystems/security modules maintain CRL).

13. As per claim 11, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the storage area stores a revocation list of illegal drive units (Traw: figure 3: CRL is available to the content source and content destination devices).

Art Unit: 2431

14. As per claim 12, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the drive unit stores a revocation list of illegal recording media (Traw: figure 4: the destination device keep CRL of illegal content sources).

15. As per claim 13, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the drive unit does not store a revocation list of illegal recording medium (Traw: figure 4: the CRL is provided to the content destination device, and is not necessarily stored in any particular area).

16. As per claim 14, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the mutual authentication protocol executes independently of whether the drive unit or the portable data recording medium contains an illegal unit revocation list (Traw: column 7 lines 44-65).

17. As per claim 15, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the controller of the drive unit judges whether or not the security module has an illegal unit revocation list stored therein, and executes the mutual authentication protocol based on the judgment (Traw: column 7 lines 15-35).

18. As per claim 17, Traw discloses the system as set forth in claim 1. Traw further discloses wherein

Art Unit: 2431

the portable data recording medium stores therein a first version of an illegal unit revocation list and a first list version number (Traw: column 7 lines 5-15: CRL version number is sent from content source/recording medium to content destination);

the drive unit stores therein a second version of the illegal unit revocation list and a second list version number (Traw: column 7 lines 30-35: the destination device also contains a CRL to compare version of the lists); and

the data recording medium and the drive unit exchange the first and second version numbers when executing the mutual authentication protocol, and whichever has a newer version of the illegal unit revocation list sends the newer version of the illegal unit revocation list to the other (Traw: column 7 lines 33-36: update the list if the other device has more recent list).

19. As per claim 18, Traw discloses the system as set forth in claim 17. Traw further discloses wherein

the portable data recording medium has the first list version number and the first version of the illegal unit revocation list stored in the storage area (Traw: column 7 lines 5-35: CRL version number);

the drive unit comprises a storage unit and stores the second list version number and the second version of the illegal unit revocation list stored in the storage unit (Traw: column 7 lines 30-35);

the security module of the portable data recording medium and controller of the drive unit exchange the first version number and the second version number when executing the mutual authentication protocol (Traw: column 7 lines 32-33: compare the version numbers); and

Art Unit: 2431

the portable data recording medium and drive unit exchange the list with the newer version number (Traw: column 7 lines 34-36: update the CRL).

20. As per claim 19, Traw discloses the system as set forth in claim 1. Traw further discloses wherein the drive unit checks a second version of an illegal unit revocation list to authenticate the security module and the security module checks a first version of the illegal unit revocation list to authenticate the drive unit (Traw: column 7 lines 30-35 and 60-65).

21. As per claim 20, Traw discloses the system as set forth in claim 17. Traw further discloses wherein:

the drive unit further stores identification data (Traw: column 6 lines 25-30: unique device ID); and

the security module receives the identification data from the drive unit and checks whether or not the identification data of the drive unit is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if the drive unit is revoked (Traw: column 7 lines 44-65: security module of the content source checks whether the content destination is valid).

22. As per claim 21, Traw discloses the system set forth in claim 17. Traw further discloses wherein:

the portable data recording medium stores identification data; and

Art Unit: 2431

the controller of the drive unit receives the identification data from the security module and checks whether or not the identification data of the portable data recording medium is registered in the illegal unit revocation list, when executing the mutual authentication protocol, and will not go through subsequent processes after execution of the mutual authentication protocol if portable data recording medium is revoked (Traw: column 7 lines 15-35).

23. As per claim 22, Traw discloses the system set forth in claim 17. Traw further discloses wherein the illegal unit revocation list includes identification data of revoked units (Traw: column 27-32: checks CRL to see if device is revoked).

24. As per claim 23, Traw discloses the system set forth in claim 17. Traw further discloses wherein the illegal unit revocation list identifies units that have not been revoked (Traw: column 7 lines 27-32).

25. As per claim 24, Traw discloses the system set forth in claim 17. Traw further discloses wherein the illegal unit revocation list includes:

a revocation list identifying revoked units (Traw: column 7 lines 27-32);

a registration list identifying units that have not been revoked,

wherein units identified by the revocation list and units not identified by the registration list are considered revoked (Traw: column 7 lines 25-27: determine whether device is compliant).

Art Unit: 2431

26. As per claim 25, Traw discloses the system set forth in claim 17. Traw further discloses wherein the illegal unit revocation list includes:

a revocation list identifying revoked units (Traw: column 7 lines 27-32);

a registration list identifying units that have not been revoked,

wherein one or more of the revocation and registration lists is used to determine whether a unit is considered revoked (Traw: column 7 lines 25-27: determine whether device is compliant).

27. As per claim 26, Traw discloses the system set forth in claim 17. Traw further discloses wherein when executing the mutual authentication protocol, the drive unit and the security module execute a key sharing protocol using public-key encryption technology, encrypt a content key with a shared key, and transfer the encrypted content key (Traw: column 5 lines 48-52).

28. As per claim 27, Traw discloses the system set forth in claim 1. Traw further discloses wherein when executing the mutual authentication protocol, the drive unit and the security module execute a key sharing protocol using public-key encryption technology, encrypt data with a shared key, and transfer the encrypted data (Traw: figure 3 and figure 4).

29. As per claim 28, Traw discloses the system set forth in claim 1. Traw further discloses wherein:

Art Unit: 2431

the drive unit is to write data to the storage area of the portable data recording medium via the interface unit;

the drive unit and the security module execute a key sharing protocol using the public-key encryption technology;

the drive unit encrypts a content key with a shared key and sends the encrypted content key to the security module; and

the security module decrypts the encrypted content key, re-encrypts the decrypted content key with a slave key stored therein and sends the re-encrypted content key to the drive unit; and

the drive unit writes to the storage area of the portable data recording medium the data encrypted with the content key and the content key encrypted by the save key (Traw: column 3 lines 45-64).

30. As per claim 29, Traw discloses the system set forth in claim 1. Traw further discloses wherein:

the drive unit is to read data from the storage area via the interface unit;

the drive unit and security module execute a key sharing protocol using public-key encryption technology;

the drive unit reads the encrypted content key from the storage area and sends the read content key to the security module;

the security module decrypts the encrypted content key received from the drive unit with a save key stored therein, re-encrypts the decrypted content key with the shared key and sends the re-encrypted content key to the drive unit; and

Art Unit: 2431

the drive unit decrypts the unencrypted content key received from the security module with the shared key, reads the content key-encrypted data from the storage area and decrypts the data (Traw: column 3 lines 45-64).

31. As per claim 30-33, claims 30-33 encompass the same scope as claims 28 and 29. Therefore, claims 30-33 are rejected based on the same reason set forth above in rejecting claims 28 and 29.

32. As per claim 34-37, 39-45, 47-69, 71-73, 75-90, and 138-157, they encompass the same scope as claims 1-7, 9-15 and 17-33. Therefore, they are rejected based on the same reason set forth above in rejecting claims 1-7, 9-15 and 17-33.

Response to Arguments

33. Applicant's remarks have been considered. The examiner has provided more detailed mapping of the prior art and claimed invention as presently amended. Therefore, argument regarding to the previous office action are not being considered at this time as they are directed toward newly amended claims.

34. On the other hand, the term "portable data storage medium" is not limited to optical disc or medium specified by the applicant. Instead, it could be interpreted to be any device that includes memory capable of being utilized by different users/systems (portable aspect).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2431

/Shin-Hon Chen/
Examiner, Art Unit 2431